CS2420

UNIVERSITY OF WARWICK

Second Year Examinations: Summer 2008

Formal Specification and Verification

Time allowed: 2 hours.

Answer **FOUR** questions.

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer booklet.

---

1. (a) Present the natural deduction rules:

   $\rightarrow$-elimination, $\neg$-introduction and $\neg$-elimination. [6]

   (b) By formulating suitable propositions, express each of the following arguments as sequents:

   i. When the sun is shining, the cat sleeps on the balcony. The cat is not sleeping on the balcony, so the sun is not shining.
   ii. When the sun is shining, the cat sleeps on the balcony. The cat is sleeping on the balcony, so the sun is shining.
   iii. When the sun is shining, the cat sleeps on the balcony. The cat is sleeping under the table, so the sun is not shining.

   [9]

   (c) Which sequents in part (b) are valid, and which are invalid? Give a formal justification for your answers, applying the rules of natural deduction where appropriate, and discussing any semantic problems you encounter. [10]

---

2. (a) What does it mean for the set of rules of a deductive system to be *sound* and to be *complete*? [6]

   (b) Outline a proof that the natural deduction rules for propositional logic are *sound*. [9]

   (c) Briefly and informally explain what is meant by the Post Correspondence Problem and how it can be used to show that the problem of determining the validity of a predicate calculus formula is undecidable. [Your explanation should highlight key concepts and principles but is not expected to include mathematical details.] [8]

   (d) Is natural deduction sound and complete for predicate logic? [2]

---

3. (a) Explain what is meant by each of the following:
   i. a *model* of predicate logic;
   ii. an *environment* with respect to a model;
   iii. that $\phi_1, \cdots, \phi_n$ *semantically entail* ψ;
   iv. that $\phi_1, \cdots, \phi_n$ are *consistent*.

[10]

(b) Suppose that R is a binary relation on a set. Write down a sequent in predicate logic that is valid if and only if R is a *transitive* relation. [5]

(c) Construct a model in which R is a transitive relation such that the following sequent is *invalid*:

$$\forall x \exists y R(x, f(y)), \forall y \exists x R(f(x), y) \vdash \forall x R(x, x)$$

[5]

(d) Construct a model to show that the following formulas are consistent with R being a transitive relation:

$$\forall x \exists y R(x, f(y)), \forall y \exists x R(f(x), y), \forall x R(x, x)$$

[5]

---

4. (a) What is meant by satisfaction of a Hoare triple $(\!|\phi|\!)\ P\ (\!|\psi|\!)$ under total correctness? [4]

(b) Explain what is meant by the *weakest precondition* for a statement S to establish a post-condition ψ. Describe techniques for finding the weakest precondition for an assignment and for an *if*-statement. In what respect is finding the weakest precondition for a *while*-statement more difficult? [6]

(c) Let `Square` denote the following code for computing the square of a positive integer:

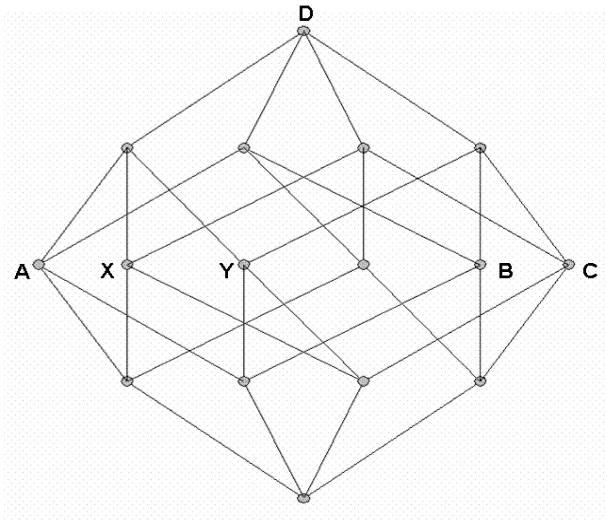
```
x = n;
z = 0;
while (x > 0) {
    z = z + n;
    x = x - 1;
}
```

Show $\vdash_{tot} (\!|n \geq 0|\!)$ `Square` $(\!|z = n \cdot n|\!)$ by a proof tableau. [12]

(d) How would you adapt the code and proof in part (c) to compute the square of any given integer? [3]

---

5. (a) A Boolean algebra is a distributive lattice in which every element has a complement. Express this characterisation formally by explicitly stating the axioms that define a Boolean algebra. [8]



(b) The above figure is a Hasse diagram that represents the set of logically distinct propositional formulas that can be constructed from atomic propositions p and q ordered by the relation $\phi \leq \psi$ if and only if $\phi \rightarrow \psi$. Given that p is represented by the point A:

i. Which of the points B and C represents the proposition q? Specify a propositional formula that is represented by the other point. [3]

ii. Which of the points X and Y represents the proposition ¬q? Specify a propositional formula that is represented by the other point. [4]

iii. What class of propositions does the point D represent? [2]

(c) Explain informally how you would use the Alloy tool to search for Boolean algebras with at most 8 elements. [3]

(d) What results would you expect your search to return, and how would these be represented graphically by Hasse diagrams? [5]